MIAMI BEACH POLICE

MEDIA RELATIONS UNIT
1100 Washington Avenue
Miami Beach, FL 33139

NEWS RELEASE

(305) 673-7383 Fax 673-7065

FOR IMMEDIATE RELEASE
Date: **January 12, 2005**
Contact: **Officer Bobby Hernandez**
Phone: 305-673-7776 Ext. 5163
PIO #: 05-04

TSUNAMI DISASTER RELIEF FRAUD ALERT

Washington, D.C. - The FBI today is alerting the public to a variety of scams currently being facilitated online involving the solicitation of additional relief funds for the victims of the recent Tsunami disaster. The FBI, through the Internet Crime Complaint Center (IC3), has received reports of websites being established purportedly to assist with collection and relief efforts. Complaints submitted to the IC3 have identified several schemes that involve both unsolicited in-coming emails (SPAM), as well as reports of responses to posted email addresses, to assist for a fee, in locating loved ones who may have been a victim of the disaster. A fraudulent relief donation website has also been detected containing an imbedded Trojan exploit which can infect the user's computer with a virus if accessed.

The FBI, in conjunction with domestic with international law enforcement and industry partners, take seriously these egregious actions and are resolved to aggressively pursuing those who would attempt to victimize philanthropic individuals.

The IC3 is cautioning citizens against participating in this type of on-line correspondence. Consistent with previous guidance on incidents of Phishing/Spoofing and Identity Theft, when considering on-line options for providing funding to this relief effort consumers should consider the following:

- Do not respond to any unsolicited (SPAM) incoming emails.
- Be skeptical of individuals claiming to be surviving victims or foreign government officials asking for help in placing large sums of money in overseas bank accounts.
- To ensure that contributions to U.S. based non-profit organizations are used for intended purposes, go directly to recognized charities and aid organizations websites, as opposed to following a link to another site.
- Attempt to verify the legitimacy of non-profit organizations by utilizing various Internet based resources which may assist in confirming the existence of the organization as well as its non-profit status.
- Be leery of emails that claim to show pictures of the disaster areas in attached files, as the files may contain viruses. Only open attachments from know senders.

Several variations of this scam are currently in circulation. Anyone who has received an email referencing the above information or anyone who may have been a victim of this or a similar incident should notify the IC3 via the website, www.ic3.gov.